CLAIMS

What is claimed is:

1. A method comprising:

selecting an elliptic curve;

determining a Squared Weil pairing based on said elliptic curve; and

cryptographically processing selected information based on said Squared Weil pairing.

2. The method as recited in Claim 1, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

3. The method as recited in Claim 2, wherein determining said Squared Weil pairing based on said elliptic curve further includes establishing a point **id** that is defined as a point at infinity on E, and wherein $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{X}$ are points on E wherein $\boldsymbol{X}$ is an indeterminate denoting an independent variable of a function, and wherein $x(\boldsymbol{X})$, $y(\boldsymbol{X})$ are functions mapping said point $\boldsymbol{X}$ on E to its affine x and y coordinates, and wherein a line passes through said points $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ if $\boldsymbol{P} + \boldsymbol{Q} + \boldsymbol{R} = \mathbf{id}$.

4. The method as recited in Claim 3, wherein when at least two of said $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ points are equal, said line is a tangent line at a common point.

5. The method as recited in Claim 3, wherein determining said Squared Weil pairing based on said elliptic curve further includes:

with a first function $f_{j,\,\mathbf{P}}$ and a second function $f_{k,\,\mathbf{P}}$ for two integers j and k, deriving a third function $f_{-j-k,\,\mathbf{P}}$ based on said first and second functions.

6. The method as recited in Claim 5, wherein $(f_{-j-k,\mathbf{P}}\, f_{j,\mathbf{P}}\, f_{k,\mathbf{P}}) = (f_{-j-k,\,\mathbf{P}}) + (f_{j,\,\mathbf{P}}) + (f_{k,\,\mathbf{P}}) = 3(\mathbf{id}) - ((-j-k)\mathbf{P}) - (j\mathbf{P}) - (k\mathbf{P})$.

7. The method as recited in Claim 5, wherein $f_{-j-k,\mathbf{P}}(\mathbf{X})\ f_{j,\mathbf{P}}(\mathbf{X})\ f_{k,\mathbf{P}}(\mathbf{X})$ $\mathrm{line}(j\mathbf{P}, k\mathbf{P}, (-j-k)\mathbf{P})(\mathbf{X})$ = a constant.

8. The method as recited in Claim 5, wherein if j is an integer and $\mathbf{P}$ a point on E, then said first and second functions are rational functions on E whose divisor of zeros and poles is $(f_{j,\mathbf{P}}) = j(\mathbf{P}) - (j\mathbf{P}) - (j-1)(\mathbf{id})$.

9. The method as recited in Claim 8, wherein if $j > 1$ and $\mathbf{P}$, $j\mathbf{P}$, and $\mathbf{id}$ are distinct, then said first function has a j-fold zero at $\mathbf{X} = \mathbf{P}$, a simple pole at $\mathbf{X} = j\mathbf{P}$, a $(j-1)$-fold pole at infinity, and no other poles or zeros.

10. The method as recited in Claim 8, wherein if j equals 0 or 1 then said first function is a nonzero constant.

11. The method as recited in Claim 5, further comprising determining $f_{0,\mathbf{P}}$ such that a line through $0\mathbf{P} = \mathbf{id}$, $(-j-k)\mathbf{P}$, and $(j+k)\mathbf{P}$ is vertical in that its equation does not reference a y-coordinate.

12. The method as recited in Claim 11, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{line}\big(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\big)(\boldsymbol{X})}{\text{line}\big(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\big)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X})\text{line}\big(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\big)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X})\text{line}\big(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\big)(\boldsymbol{X})}.$$

13. The method as recited in Claim 11, wherein:

$f_{j,\,\boldsymbol{id}}$ = constant;

$f_{j,\,-\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\,\boldsymbol{P}}(-\boldsymbol{X})$*(constant); and

if ($\boldsymbol{P}+\boldsymbol{Q}+\boldsymbol{R} = \mathbf{id}$), then:

$$f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{Q}}(\boldsymbol{X}) f_{j,\boldsymbol{R}}(\boldsymbol{X}) = \frac{\text{line}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{R})(\boldsymbol{X})^j}{\text{line}(j\boldsymbol{P}, j\boldsymbol{Q}, j\boldsymbol{R})(\boldsymbol{X})}.$$

14. The method as recited in Claim 3, wherein $\boldsymbol{P}$ and $\boldsymbol{Q}$ are m-torsion points on E and m is an odd prime, and wherein determining said Squared Weil pairing further includes:

determining said squared Weil pairing based on

$$\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(\boldsymbol{P})} = -e_m(\boldsymbol{P},\boldsymbol{Q})^2,$$

where e_m denotes the Weil-pairing.

15. The method as recited in Claim 14, wherein neither $\boldsymbol{P}$ nor $\boldsymbol{Q}$ is an identity and $\boldsymbol{P}$ is not equal to $\pm\boldsymbol{Q}$.

16. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil pairing based on an elliptic curve; and

cryptographically processing selected information based on said Squared Weil pairing.

17. The computer-readable medium as recited in Claim 16, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

18. The computer-readable medium as recited in Claim 17, determining said Squared Weil pairing based on said elliptic curve further includes establishing a point **id** that is defined as a point at infinity on E, and wherein $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{X}$ are points on E wherein $\boldsymbol{X}$ is an indeterminate denoting an independent variable of a function, and wherein $x(\boldsymbol{X})$, $y(\boldsymbol{X})$ are functions mapping said point $\boldsymbol{X}$ on E to its affine x and y coordinates, and wherein a line passes through said points $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ if $\boldsymbol{P} + \boldsymbol{Q} + \boldsymbol{R} = \mathbf{id}$.

19. The computer-readable medium as recited in Claim 18, wherein determining said Squared Weil pairing based on said elliptic curve further includes:

determining a first function $f_{j,\boldsymbol{P}}$ and a second function $f_{k,\boldsymbol{P}}$ for two integers j and k; and

determining a third function $f_{-j-k,\boldsymbol{P}}$ based on said first and second functions.

20. The computer-readable medium as recited in Claim 19, wherein $(f_{-j-k,\boldsymbol{P}}\ f_{j,\boldsymbol{P}}\ f_{k,\boldsymbol{P}}) = (f_{-j-k,\boldsymbol{P}}) + (f_{j,\boldsymbol{P}}) + (f_{k,\boldsymbol{P}}) = 3(\mathbf{id}) - ((-j-k)\boldsymbol{P}) - (j\boldsymbol{P}) - (k\boldsymbol{P})$.

21. The computer-readable medium as recited in Claim 20, wherein $f_{-j-k,\boldsymbol{P}}(\boldsymbol{X})\ f_{j,\boldsymbol{P}}(\boldsymbol{X})\ f_{k,\boldsymbol{P}}(\boldsymbol{X})\ \mathrm{line}(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P})(\boldsymbol{X})$ = a constant.

22. The computer-readable medium as recited in Claim 20, wherein if j is an integer and $\boldsymbol{P}$ a point on E, then said first and second functions *are* rational functions on E whose divisor of zeros and poles is $(f_{j,\boldsymbol{P}}) = j(\boldsymbol{P}) - (j\boldsymbol{P}) - (j-1)(\mathbf{id})$.

23. The computer-readable medium as recited in Claim 20, further comprising determining $f_{0,\boldsymbol{P}}$ such that a line through $0\boldsymbol{P} = \mathbf{id}$, $(-j-k)\boldsymbol{P}$, and $(j+k)\boldsymbol{P}$ is vertical in that it does not reference a y-coordinate.

24. The computer-readable medium as recited in Claim 23, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\mathrm{line}\big(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\big)(\boldsymbol{X})}{\mathrm{line}\big(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\big)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X})\mathrm{line}\big(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\big)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X})\mathrm{line}\big(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\big)(\boldsymbol{X})}.$$

25. The computer-readable medium as recited in Claim 23, wherein:

$f_{j,\mathbf{id}}$ = constant;

$f_{j,-\mathbf{P}}(\mathbf{X}) = f_{j,\mathbf{P}}(-\mathbf{X})$*(constant); and

if ($\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{id}$), then:

$$f_{j,\mathbf{P}}(\mathbf{X})f_{j,\mathbf{Q}}(\mathbf{X})f_{j,\mathbf{R}}(\mathbf{X}) = \frac{\text{line}(\mathbf{P},\mathbf{Q},\mathbf{R})(\mathbf{X})^j}{\text{line}(j\mathbf{P},j\mathbf{Q},j\mathbf{R})(\mathbf{X})}.$$

26. The computer-readable medium as recited in Claim 18, wherein $\mathbf{P}$ and $\mathbf{Q}$ are m-torsion points on E and m is an odd prime, and wherein determining said Squared Weil pairing further includes:

determining said squared Weil pairing based on

$$\frac{f_{m,\mathbf{P}}(\mathbf{Q})f_{m,\mathbf{Q}}(-\mathbf{P})}{f_{m,\mathbf{P}}(-\mathbf{Q})f_{m,\mathbf{Q}}(\mathbf{P})} = -e_m(\mathbf{P},\mathbf{Q})^2,$$

where e_m denotes the Weil-pairing.

27. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to said memory and configured to determine a Squared Weil pairing based on at least one elliptic curve, and cryptographically process selected information stored in said memory based on said Squared Weil pairing.

28. The apparatus as recited in Claim 27, wherein said logic is further configured to determine said elliptic curve, which includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

29. The apparatus as recited in Claim 27, wherein said logic is further configured to establishing a point **id** that is defined as a point at infinity on E, and wherein $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{X}$ are points on E wherein $\boldsymbol{X}$ is an indeterminate denoting an independent variable of a function, and wherein $x(\boldsymbol{X})$, $y(\boldsymbol{X})$ are functions mapping said point $\boldsymbol{X}$ on E to its affine x and y coordinates, and wherein a line passes through said points $\boldsymbol{P}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ if $\boldsymbol{P} + \boldsymbol{Q} + \boldsymbol{R} = \mathbf{id}$.

30. The apparatus as recited in Claim 29, wherein said logic is further configured to determine a first function $f_{j,\boldsymbol{P}}$ and a second function $f_{k,\boldsymbol{P}}$ for two integers j and k, and a third function $f_{-j-k,\boldsymbol{P}}$ based on said first and second functions.

31. The apparatus as recited in Claim 30, wherein $(f_{-j-k,\boldsymbol{P}}\ f_{j,\boldsymbol{P}}\ f_{k,\boldsymbol{P}}) = (f_{-j-k,\boldsymbol{P}}) + (f_{j,\boldsymbol{P}}) + (f_{k,\boldsymbol{P}}) = 3(\mathbf{id}) - ((-j-k)\boldsymbol{P}) - (j\boldsymbol{P}) - (k\boldsymbol{P})$.

32. The apparatus as recited in Claim 30, wherein $f_{-j-k,\boldsymbol{P}}(\boldsymbol{X})\, f_{j,\boldsymbol{P}}(\boldsymbol{X})\, f_{k,\boldsymbol{P}}(\boldsymbol{X})\, \mathrm{line}(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P})(\boldsymbol{X})$ = a constant.

33. The apparatus as recited in Claim 30, wherein if j is an integer and $\boldsymbol{P}$ a point on E, then said first and second functions are rational functions on E whose divisor of zeros and poles is $(f_{j,\boldsymbol{P}}) = j(\boldsymbol{P}) - (j\boldsymbol{P}) - (j-1)(\mathbf{id})$.

34. The apparatus as recited in Claim 30, wherein said logic is further configured to determine $f_{0,\boldsymbol{P}}$ such that a line through $0\boldsymbol{P} = \mathbf{id}$, $(-j-k)\boldsymbol{P}$, and $(j+k)\boldsymbol{P}$ is vertical in that it does not reference a y-coordinate.

35. The apparatus as recited in Claim 34, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{line}\left(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\right)(\boldsymbol{X})}{\text{line}\left(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\right)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X}) line\left(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\right)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X}) line\left(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\right)(\boldsymbol{X})}.$$

36. The apparatus as recited in Claim 34, wherein:

$f_{j,\mathbf{id}}$ = constant;

$f_{j,-\boldsymbol{P}})(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(-\boldsymbol{X})$*(constant); and

if $(\boldsymbol{P} + \boldsymbol{Q} + \boldsymbol{R} = \mathbf{id})$, then:

$$f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{Q}}(\boldsymbol{X}) f_{j,\boldsymbol{R}}(\boldsymbol{X}) = \frac{\text{line}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{R})(\boldsymbol{X})^j}{\text{line}(j\boldsymbol{P}, j\boldsymbol{Q}, j\boldsymbol{R})(\boldsymbol{X})}.$$

37. The apparatus as recited in Claim 30, wherein $\boldsymbol{P}$ and $\boldsymbol{Q}$ are m-torsion points on E and m is an odd prime, and wherein said logic is further configured to determine said squared Weil pairing based on

$$\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(\boldsymbol{P})} = -e_m(\boldsymbol{P},\boldsymbol{Q})^2,$$

where e_m denotes the Weil-pairing.

38. A method comprising:

determining a Squared Weil Pairing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$ by:

establishing an odd prime m on a curve E*; and*

based on two m-torsion points $\boldsymbol{P}$ and $\boldsymbol{Q}$ on E, computing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$.

39. The method as recited in Claim 38, further comprising forming a mathematical chain for m.

40. The method as recited in Claim 39, wherein said mathematical chain is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

41. The method as recited in Claim 39, wherein in forming said mathematical chain for m, every element in said mathematical chain is a sum or difference of two earlier elements in said mathematical chain, which continues until m is included in said mathematical chain.

42. The method as recited in Claim 41, wherein said mathematical chain has a length O(log(m)).

43. The method as recited in Claim 39, wherein for each j in said mathematical chain, a tuple $t_j = [j\boldsymbol{P}, j\boldsymbol{Q}, n_j, d_j]$ is formed such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})f_{j,}\ (\boldsymbol{P})}.$$

44. The method as recited in Claim 43, wherein determining said Squared Weil Pairing further includes:

starting with $t_1 = [\boldsymbol{P}, \boldsymbol{Q}, 1, 1]$, given t_j and t_k, determine t_{j+k} by:

forming elliptic curve sums: $j\boldsymbol{P} + k\boldsymbol{P} = (j+k)\boldsymbol{P}$ and $j\boldsymbol{Q} + k\boldsymbol{Q} = (j+k)\boldsymbol{Q}$;

determining $\mathrm{line}(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P})(\boldsymbol{X}) = c0 + c1*x(\boldsymbol{X}) + c2*y(\boldsymbol{X})$;

determining $\mathrm{line}(j\boldsymbol{Q}, k\boldsymbol{Q}, (-j-k)\boldsymbol{Q})(\boldsymbol{X}) = c0' + c1'*x(\boldsymbol{X}) + c2'*y(\boldsymbol{X})$;

and

setting

$$n_{j+k} = n_j*n_k* (c0 + c1*x(\boldsymbol{Q}) + c2*y(\boldsymbol{Q})) * (c0' + c1'*x(\boldsymbol{P}) - c2'*y(\boldsymbol{P}))$$

and

$$d_{j+k} = d_j*d_k* (c0 + c1*x(\boldsymbol{Q}) - c2*y(\boldsymbol{Q})) * (c0' + c1'*x(\boldsymbol{P}) + c2'*y(\boldsymbol{P})).$$

45. The method as recited in Claim 44, further comprising determining t_{j+k} from t_j and t_k, wherein vertical lines through $(j+k)\boldsymbol{P}$ and $(j+k)\boldsymbol{Q}$ do not appear in said formulae for n_{j+k} and d_{j+k} when contributions from $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ are equal, and wherein $-\boldsymbol{Q}$ is the complement of $\boldsymbol{Q}$ and when contributions from $\boldsymbol{P}$ and $-\boldsymbol{P}$ are equal, and wherein $-\boldsymbol{P}$ is the complement of $\boldsymbol{P}$.

46. The method as recited in Claim 44, wherein if $j + k = m$, then $n_{j+k} = n_j * n_k$ and $d_{j+k} = d_j * d_k$.

47. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil Pairing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$ by:

establishing an odd prime m on a curve E; and

based on two m-torsion points $\boldsymbol{P}$ and $\boldsymbol{Q}$ on E, computing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$.

48. The computer-readable medium as recited in Claim 47, further comprising forming a mathematical chain for m selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain, such that every element in said mathematical chain is a sum or difference of two earlier elements in said mathematical chain, which continues until m is included in said mathematical chain.

49. The computer-readable medium as recited in Claim 48, wherein for each j in said mathematical chain, a tuple $t_j = [j\boldsymbol{P}, j\boldsymbol{Q}, n_j, d_j]$ is formed such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})f_{j,\boldsymbol{Q}}(\boldsymbol{P})}.$$

50. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to said memory and configured to determine a Squared Weil Pairing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$ by establishing an odd prime m on a curve E, and based on two m-torsion points $\boldsymbol{P}$ and $\boldsymbol{Q}$ on E, computing $e_m(\boldsymbol{P}, \boldsymbol{Q})^2$.

51. The apparatus as recited in Claim 50, wherein said logic is further configured to form a mathematical chain for m that is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

52. The apparatus as recited in Claim 51, wherein for each j in said mathematical chain, said logic is further configured to form a tuple $t_j = [j\boldsymbol{P}, j\boldsymbol{Q}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})f_{j,\boldsymbol{Q}}(\boldsymbol{P})}.$$

53. A method comprising:

determining a Squared Weil pairing $(m, \boldsymbol{P}, \boldsymbol{Q})$, where m is an odd prime number, by setting $t_1 = [\boldsymbol{P}, \boldsymbol{Q}, 1, 1]$, using an addition-subtraction chain to determine $t_m=[m\boldsymbol{P}, m\boldsymbol{Q}, n_m, d_m]$, and if n_m and d_m are nonzero, then determining:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \text{ and}$$

cryptographically processing selected information based on said Squared Weil pairing.

54. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil pairing (m, $\boldsymbol{P}$, $\boldsymbol{Q}$), where m is an odd prime number, by setting t_1 = [$\boldsymbol{P}$, $\boldsymbol{Q}$, 1, 1], using an addition-subtraction chain to determine t_m=[$m\boldsymbol{P}$, $m\boldsymbol{Q}$, n_m, d_m], and if n_m and d_m are nonzero, then determining:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \text{ and}$$

cryptographically processing selected information based on said Squared Weil pairing.

55. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to said memory and configured to:

determine a Squared Weil pairing (m, $\boldsymbol{P}$, $\boldsymbol{Q}$), where m is an odd prime number, by setting t_1 = [$\boldsymbol{P}$, $\boldsymbol{Q}$, 1, 1],

use an addition-subtraction chain to determine t_m=[$m\boldsymbol{P}$, $m\boldsymbol{Q}$, n_m, d_m],

if n_m and d_m are nonzero, then determine

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \text{ and}$$

cryptographically process selected information based on said Squared Weil pairing.

56. A method comprising:

selecting an elliptic curve;

determining a Squared Tate pairing based on said elliptic curve; and

cryptographically processing selected information based on said Squared Tate pairing.

57. The method as recited in Claim 56, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

58. The method as recited in Claim 56, wherein m is an odd prime on K and P is an m-torsion point on E, Q is a point on E, with neither $\boldsymbol{P}$ nor $\boldsymbol{Q}$ being the identity and wherein $\boldsymbol{P}$ is not equal to a multiple of $\boldsymbol{Q}$, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P},\boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing.

59. The method as recited in Claim 56, wherein determining said Squared Tate pairing includes determining $v_m(\boldsymbol{P}, \boldsymbol{Q})$ by:

establishing an odd prime m and said elliptic curve E;

given an m-torsion point $\boldsymbol{P}$ on E and a point $\boldsymbol{Q}$ on E, determining a mathematical chain for m; and

for each j in said mathematical chain, forming a tuple $t_j = [j\boldsymbol{P}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})}.$$

60. The method as recited in Claim 59, further comprising:

starting with $t_1 = [\boldsymbol{P}, 1, 1]$, given t_j and t_k, determining t_{j+k} by:

forming an elliptic curve sum $j\boldsymbol{P} + k\boldsymbol{P} = (j+k)\boldsymbol{P}$,

determining $\text{line}(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P})(\boldsymbol{X}) = c0 + c1*x(\boldsymbol{X}) + c2*y(\boldsymbol{X})$, and

setting: $n_{j+k} = n_j * n_k * (c0 + c1*x(\boldsymbol{Q}) + c2*y(\boldsymbol{Q}))$ and

$d_{j+k} = d_j * d_k * (c0 + c1*x(\boldsymbol{Q}) - c2*y(\boldsymbol{Q}))$.

61. The method as recited in Claim 60 further comprising determining t_{j-k} from t_j and t_k.

62. The method as recited in Clam 61, wherein if $j+k=m$, then:

$n_{j+k} = n_j * n_k$ and $d_{j+k} = d_j * d_k$.

63. The method as recited in Claim 61, wherein if n_m and d_m are nonzero, then:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}.$$

64. The method as recited in Claim 56, wherein said mathematical chain is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

65. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Tate pairing based on an elliptic curve; and

cryptographically processing selected information based on said Squared Tate pairing.

66. The computer-readable medium as recited in Claim 65, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

67. The computer-readable medium as recited in Claim 65, wherein m is an odd prime on K and P is an m-torsion point on E, $\boldsymbol{Q}$ is a point on E, with neither $\boldsymbol{P}$ nor $\boldsymbol{Q}$ being the identity and wherein $\boldsymbol{P}$ is not equal to a multiple of $\boldsymbol{Q}$, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P},\boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing.

68. The computer-readable medium as recited in Claim 65, wherein determining said Squared Tate pairing includes determining $v_m(\boldsymbol{P}, \boldsymbol{Q})$ by:

establishing an odd prime m and said elliptic curve E;

given an m-torsion point $\boldsymbol{P}$ on E and a point $\boldsymbol{Q}$ on E, determining a mathematical chain for m; and

for each j in said mathematical chain, forming a tuple $t_j = [j\boldsymbol{P}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})}.$$

69. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to said memory and configured to determine a Squared Tate pairing based on an elliptic curve; and

cryptographically processing selected information based on said Squared Tate pairing.

70. The apparatus as recited in Claim 69, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

71. The apparatus as recited in Claim 69 wherein m is an odd prime on K and P is an m-torsion point on E, $\boldsymbol{Q}$ is a point on E, with neither $\boldsymbol{P}$ nor $\boldsymbol{Q}$ being the identity and wherein $\boldsymbol{P}$ is not equal to a multiple of $\boldsymbol{Q}$, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P},\boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing.

72. The apparatus as recited in Claim 69, wherein said logic is further configured to:

establish an odd prime m and said elliptic curve E;

given an m-torsion point $\mathbf{P}$ on E and a point $\mathbf{Q}$ on E, determine a mathematical chain for m; and

for each j in said mathematical chain, form a tuple $t_j = [j\mathbf{P}, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\mathbf{P}}(\mathbf{Q})}{f_{j,\mathbf{P}}(-\mathbf{Q})}.$$